

Third-party security: Who can you trust?

By Jay Cline

April 1, 2003 12:00 PM ET

The largest security breach in history—combined with a host of new privacy laws—is spurring companies to scrutinize third-party data processors like never before. Sound like a positive development? Not entirely. It has turned into a massive witch hunt for security holes, resulting in untold losses in productivity throughout corporate America. The fire drill comes at a time when companies struggling to stay in the black can hardly afford a diversion of resources that doesn't deliver an equivalent value.

Everyone who works in security saw the headlines last month: "Data processor hacked; 8 million credit card numbers exposed." The massive breach at Data Processors International (DPI) reverberated in boardrooms and cubicles across the country. Companies began asking the question that won't go away: Are we truly safe giving our data to our business partners?

The DPI breach comes on the heels of numerous new privacy laws requiring companies to hold their business partners accountable to their own security standards. European, Canadian and Australian privacy laws include this tenet, as do America's own privacy statutes for the financial services and health care industries. Companies that don't manage the risks of data held by their partners face increasing exposure to fines and lawsuits.

So how are corporations responding? In the pre-Internet days, companies were satisfied with receiving contractual indemnification from their business

partners—meaning the partners would be responsible for any damages caused by security breaches that were their own fault. But third parties can't repair the damage to a client's brand following a security breach. Indemnification is no longer enough to establish third-party security.

As a result, firms whose reputations are at stake are now subjecting their data partners to a battery of tests aimed at ensuring that the partners can actually meet their security obligations. This due-diligence gauntlet can include an encyclopedic security survey, a comprehensive site audit and ongoing penetration testing. The results are extremely valuable for both sides—assurance for the client, and quality improvement for the supplier.

But this path to third-party security isn't cheap. A single security review can involve multiple people on both sides for up to a month. Several companies are now assigning full-time personnel whose only jobs are to conduct and respond to third-party security reviews. The labor impact is significant, because every company is re-creating its own security standards and propagating them through its supply chains. As many as a hundred different sets of corporate security standards are now traversing the cubicles of America.

So how do we get the same level of assurance from our business partners but at a lower cost? I have a one-word answer: standardization. The information security officers of America's major regulated companies need to schedule a summit in Peoria and agree on a common set of categories for assessing organizational security.

Using the same lexicon and metrics, business partners could build boilerplate descriptions of their security practices for prospective clients. Weeks and months of effort per security review would shrink to hours on both sides. Widespread adoption of a common security terminology would also reduce the time and cost needed for external auditors to do their duties.

The good news is that this security terminology has already been developed. In the early 1990s, the security officers at several British multinationals created what has become an ISO standard for security, ISO/IEC 17799. Citibank, Sony and Unisys have been certified under the standard, and the governments of Hong Kong, Taiwan and Singapore are reportedly requiring companies to receive this certification before doing electronic business with them. The standard's vague definitions need much refinement, but they're a sufficient starting point for American businesses seeking to save overhead.

Our British friends have done good work, and we should follow their lead. The next time you engage a data partner, measure them against the 17799.